REMARKS

In the Office Action,[1] the Examiner rejected claim 14 under 35 U.S.C. § 101 as being directed to nonstatutory subject matter; and rejected claims 9 and 14 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,537,314 to Kanter ("*Kanter*") in view of U.S. Patent No. 6,594,640 to Postrel ("*Postrel*"), U.S. Publication No. 2001/0037453 to Mitty et al. ("*Mitty*"), and U.S. Patent No. 6,718,468 to Challener et al. ("*Challener*").

Applicant respectfully traverses the rejection of claim 14 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. However, to advance prosecution, Applicant amends claim 14 to recite "redeeming, using a processing, the points." Claim 14 further recites "the points . . . being managed in a point account stored in a point account database." For at least these reasons, the method of claim 14 is tied to a particular machine, and thus claim 14 is directed to statutory subject matter. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claim 14 under 35 U.S.C. § 101.

Applicant respectfully traverses the rejection of claims 9 and 14 under 35 U.S.C. § 103(a) as unpatentable over *Kanter* in view of *Postrel*, *Mitty*, and *Challener*.

Claim 14 recites a method comprising, for example, "issuing a user certificate including a hash value of a public key of the customer encrypted using a private key of a user certificate system" and "transmitting first data from the customer to a point

[1] The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement of characterization in the Office Action.

redemption system, the first data being encrypted using a public key of the point redemption system, the first data comprising a user registration request and second data including a random password and a customer account number, the second data being encrypted using a private key of the customer."

Kanter discloses, "computer 24 may verify that the participant's personal security number matches a code stored on the card, in memory 30, or within center 12, to verify that the user is authorized on that card." *Kanter*, col. 18, line 65 to col. 19, line 1. However, *Kanter* is completely silent with respect to any "encrypt[ion]," "hash value," "public key," or "private key." Accordingly, *Kanter* fails to teach or suggest "issuing a user certificate including a hash value of a public key of the customer encrypted using a private key of a user certificate system," as recited in claim 14.

Kanter also fails to teach or suggest "transmitting first data from the customer to a point redemption system, the first data being encrypted using a public key of the point redemption system, the first data comprising a user registration request and second data including a random password and a customer account number, the second data being encrypted using a private key of the customer," as recited in claim 14, at least because *Kanter* is completely silent with respect to any "encrypt[ion]," "public key," or "private key."

Postrel discloses, "interface would allow a user to login using the frequent flyer account information or preferably, the trading server account login id and password." *Postrel*, col. 11, ll. 62-64. However, *Postrel* is completely silent with respect to any "encrypt[ion]," "certificate," "hash value," "public key," or "private key." Therefore, *Postrel* fails to teach or suggest "issuing a user certificate including a hash value of a

public key of the customer encrypted using a private key of a user certificate system" and "transmitting first data from the customer to a point redemption system, the first data being encrypted using a public key of the point redemption system, the first data comprising a user registration request and second data including a random password and a customer account number, the second data being encrypted using a private key of the customer," as recited in claim 14. *Postrel* thus fails to cure the deficiencies of *Kanter*.

Mitty discloses, in reference to Fig. 6, "envelopedData 605 is the outer envelope," "core contents of envelopedData 605 is signedData 610," "core contents of signedData 610 is multipart/mixed message 615," "core contents of multipart/mixed message 615 are a plain section 620 and another envelopedData structure 625," "core contents of envelopedData structure 625 is another signedData structure 630," and "core contents of signedData 630 is valued content 635." *Mitty*, paras. 0140-45. *Mitty* further discloses "plain section 620 contained the waybill information" and "valued contents 635 . . . included the text message that the sender 105 desired to send." *Id.*, paras. 0143, 0146.

However, envelopedData 605 of *Mitty* (nor any of its inner envelopes) "includ[es] a hash value of a public key," as recited in claim 1. Although *Mitty* discloses that "[t]o get signedData 610 from envelopedData 605, the appropriate decryption techniques must be applied . . . [for] example[] . . . using the recipient's private key," para. 0140, and "decrypting . . . using the originator's public key," para. 0152, "a hash value of a public key" is not stored in envelopedData 605. Therefore, envelopedData 605 of *Mitty* cannot constitute the claimed "user certificate."

In addition, *Mitty* discloses that "plain section 620 contained the waybill information," para. 0143, not "a user registration request," as recited in claim 14. Furthermore, *Mitty* discloses that "valued contents 635 . . . included the text message that the sender 105 desired to send," para. 0146, not "a random password and a customer account number," as recited in claim 14. Therefore, envelopedData 605 of *Mitty* cannot constitute the claimed "first data."

Furthermore, *Mitty* discloses, in reference to Fig. 7, "core contents of envelopedData 705 is multipart/mixed message 710," "core contents of multipart/report 710 are . . . message 715 . . . reflecting the results of the processing; . . . message 720 . . . reflecting the results of the processing; . . . [and] message 725," including "exemplary message 730." *Mitty*, paras. 0161-67.

However, envelopedData 705 of *Mitty* does not "includ[e] a hash value of a public key," as recited in claim 14. Therefore, envelopedData 705 of *Mitty* cannot constitute the claimed "user certificate." Furthermore, envelopedData 705 of *Mitty* does not include "a user registration request" and "a random password and a customer account number," as recited in claim 14. Therefore, envelopedData 705 of *Mitty* cannot constitute the claimed "first data,"

Accordingly, *Mitty* fails to teach or suggest "issuing a user certificate including a hash value of a public key of the customer encrypted using a private key of a user certificate system" and "transmitting first data from the customer to a point redemption system, the first data being encrypted using a public key of the point redemption system, the first data comprising a user registration request and second data including a random password and a customer account number, the second data being encrypted

using a private key of the customer," as recited in claim 14. *Mitty* thus fails to cure the deficiencies of *Kanter* and *Postrel*.

Challener discloses that "a first password is generated by hashing a first pass phrase" and "a second password is generated by hashing a second pass phrase." *Challener*, col. 2, ll. 39-40 and 45-46. *Challener* further discloses several public keys and private keys. However, *Challener* does not disclose hashing any public keys. *Challener* thus cannot teach or suggest "a hash value of a public key," as recited in claim 14. Therefore, *Challener* fails to teach or suggest "issuing a user certificate including a hash value of a public key of the customer encrypted using a private key of a user certificate system," as recited in claim 14.

Challener further discloses that "the random password is encrypted along with the first password," col. 2, ll. 40-41, "[t]he random password is . . . encrypted along with the second password," col. 2, ll. 46-48, and "the random password is . . . encrypted along with the user public/private key pair," col. 4, ll. 20-21. However, *Challener* does not disclose that the random password is encrypted along with "a customer account number," as recited in claim 14. Therefore, *Challener* fails to teach or suggest "second data including a random password and a customer account number, the second data being encrypted using a private key of the customer," as recited in claim 14.

Furthermore, *Challener* discloses that "[t]he random password is . . . encrypted . . . utilizing the chip public key." *Challener*, col. 2, ll. 46-48. However, *Challener* does not disclose encrypting the encrypted random password, i.e., double encryption. Therefore, *Challener* fails to teach or suggest "first data being encrypted using a public key . . . , the first data comprising . . . second data including a random password . . . ,

the second data being encrypted using a private key," as recited in claim 14. Accordingly, *Challener* fails to teach or suggest "transmitting first data from the customer to a point redemption system, the first data being encrypted using a public key of the point redemption system, the first data comprising a user registration request and second data including a random password and a customer account number, the second data being encrypted using a private key of the customer," as recited in claim 14. *Challener* thus fails to cure the deficiencies of *Kanter*, *Postrel*, and *Mitty*.

Accordingly, a *prima facie* case of obviousness has not been established with respect to claim 14. Claim 9, although different in scope from claim 14, is allowable for at least similar reasons as claim 14. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claims 9 and 14 under 35 U.S.C. § 103(a).

In view of the foregoing, Applicant respectfully requests reconsideration of this application and timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: June 30, 2009

By: Pete Yi
Peter C. Yi
Reg. No. 61,790
202.408.4485